FORM PTO-1390 (REV. 5-93) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE **TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371**	ATTORNEY'S DOCKET NUMBER **2345/150** U.S. APPLICATION NO. (If known, see 37 CFR 1.5) 09/807235

INTERNATIONAL APPLICATION NO. **PCT/EP99/06187**	INTERNATIONAL FILING DATE **23 August 1999** **(23.08.99)**	PRIORITY DATE CLAIMED: **09 October 1998** **(09.10.98)**

TITLE OF INVENTION
A METHOD FOR GENERATING DIGITAL WATERMARKS FOR ELECTRONIC DOCUMENTS

APPLICANT(S) FOR DO/EO/US
Joerg SCHWENK and Friedrich TOENSING

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) UNSIGNED.
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☒ A substitute specification and marked-up version of specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report, Preliminary Examination Report, and Form PCT/RO/101.

U.S. APPLICATION NO (if known, see 37 C.F.R 1.5 09/807235	INTERNATIONAL APPLICATION NO PCT/EP99/06187	ATTORNEY'S DOCKET NUMBER 2345/150

17. ☒ The following fees are submitted:

Basic National Fee (37 CFR 1.492(a)(1)-(5)):

Search Report has been prepared by the EPO or JPO $860.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) $690.00

No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $710.00

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $1,000.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $100.00

				CALCULATIONS	PTO USE ONLY
ENTER APPROPRIATE BASIC FEE AMOUNT =				$ 860	
Surcharge of $130.00 for furnishing the oath or declaration later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				$	
Claims	Number Filed	Number Extra	Rate		
Total Claims	5 - 20 =	0	X $18.00	$	
Independent Claims	2 - 3 =	0	X $80.00	$	
Multiple dependent claim(s) (if applicable)			+ $270.00	$	
TOTAL OF ABOVE CALCULATIONS =				$860	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$860	
Processing fee of $130.00 for furnishing the English translation later the □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$860	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$860	
				Amount to be refunded	$
				charged	$

a. □ A check in the amount of $__________________ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of $860.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

(Reg. No. 36094)
SIGNATURE

Richard L. Mayer, Reg. No. 22,490
NAME

9 April 2001
DATE

SEND ALL CORRESPONDENCE TO:
Kenyon & Kenyon
One Broadway
New York, New York 10004
Telephone No. (212)425-7200
Facsimile No. (212)425-5288
CUSTOMER NO. 26646

26646
PATENT TRADEMARK OFFICE

[2345/150]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s) : Joerg SCHWENK et al.

Serial No. : To Be Assigned

Filed : Herewith

For : METHOD FOR GENERATING DIGITAL WATERMARKS FOR ELECTRONIC DOCUMENTS

Examiner : To Be Assigned

Art Unit : To Be Assigned

Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

SIR:

Kindly amend the above-identified application before examination, as set forth below.

IN THE TITLE:

Please replace the title with the following:

--METHOD FOR GENERATING DIGITAL WATERMARKS FOR ELECTRONIC DOCUMENTS--.

IN THE SPECIFICATION:

Please amend the specification, including abstract, pursuant to the attached substitute specification. Also attached is a marked up copy of the specification, indicating deleted and added sections. No new matter has been added.

IN THE CLAIMS:

Please cancel original claims 1 and 2, without prejudice. Please also cancel, without prejudice, claims 1-3 in the annex to the International Preliminary Examination Report.

Please add the following new claims:

4. (New) A method for generating a digital watermark for an electronic document, comprising:

determining a first hash value of the document;

generating the watermark as a function of a proof of identity id and the first hash value of the document;

providing a secret key for making the watermark visible;

embedding the watermark in the document;

restoring the document to an original state by removing the watermark using the secret key;

determining a hash value of the restored document; and

verifying ownership of the document by comparing the hash value of the restored document and the first hash value.

5. (New) The method as recited in claim 4, wherein the generating the watermark step includes generating the watermark as a function of the proof of identity id, the first hash value of the document, and an authentic time stamp.

6. (New) The method as recited in claim 5, wherein the authentic time stamp defines an embedding sequence.

7. (New) The method according to claim 4, wherein the embedding step includes embedding a plurality of different watermarks in the document, and wherein the restoring step includes restoring the document to the original state by removing all of the different watermarks, the method further comprising:

determining an original owner by comparing respective hash values in each of the different watermarks with the hash value of the restored document.

8. (New) The method according to claim 7, wherein the restoring step includes restoring the document to the original state by removing all of the different watermarks in accordance with an embedding sequence.

REMARKS

This Preliminary Amendment cancels, without prejudice, original claims 1 and 2. This Preliminary Amendment further cancels claims 1-3 in annex of the International Preliminary Examination Report, without prejudice. The new claims conform the claims to U.S. Patent and Trademark Office rules and do not add new matter to the application.

The amendments to the specification and abstract reflected in the substitute specification are to conform the specification and abstract to U.S. Patent and Trademark Office rules, and do not introduce new matter into the application.

The underlying PCT Application No. PCT/EP99/06187 includes an International Search Report, issued January 12, 2000, a copy of which is included. The Search Report includes a list of documents that were considered by the Examiner in the underlying PCT application.

The underlying PCT Application No. PCT/EP99/06187 also includes an International Preliminary Examination Report, issued November 21, 2000,. A translation of the International Preliminary Examination Report and annex thereto is included herewith.

It is respectfully submitted that the present invention is new, non-obvious, and useful. Prompt consideration and allowance of the claims are respectfully requested.

Respectfully Submitted,

KENYON & KENYON

(Reg. No. 32098)

Dated: 9 April 2001

By:

Richard L. Mayer
Reg. No. 22,490

One Broadway
New York, NY 10004
(212) 425-7200
(212) 425-5288
CUSTOMER NO. 26646

[2345/150]

A METHOD FOR GENERATING DIGITAL WATERMARKS FOR ELECTRONIC DOCUMENTS

Field of the Invention

The present invention is directed to a method for generating digital watermarks for electronic documents.

Background Information

Documents which exist in electronic form can be copied as often as desired without loss of quality. For that reason, reliable methods must be employed to prevent such documents from being freely disseminated without control, in order to protect the rights of the intellectual property owner.

Due to the rapid growth of the Internet and the capability it provides for digitally disseminating documents, there is an increased requirement to protect against the illegal dissemination of documents and, thus, to protect a copyright owner from pirated copies.

For this reason, large firms, such as IBM, NEC and Microsoft, and smaller firms as well, such as Digimarc (see Funkschau 17/97; p. 21) and research institutes, such as the Fraunhofer Company IGD and the GMD Darmstadt, have worked on embedding so-called digital watermarks in documents. In methods having such a basis, information identifying the copyright owner is introduced as invisible information into the documents to be protected. It is hidden in the document in such a way that no outsider can discover it. Only the owner himself can make the watermark visible by using his secret key and, therefore, in the case of a legal dispute, for example, prove that he is actually the owner.

There can be different kinds of inserted digital watermarks and, in this context, each can depend on the particular type of document (e.g., postscript, JPEG, MPEG-1).

Thus, for example, Schneider, M. et al., in the essay: "ROBUST CONTENT BASED DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION" in Proc. Intl. Conference on Image Processing (ICIP) New York, U.S., IEEE, 1996, pp. 227-230, describe a method for embedding digital signatures as hidden signatures into the useful data for verifying the authenticity of data, i.e., proving that the data have been manipulated with, in that signatures are extracted using hash functions, and the result is combined with a private key, so that, altogether, a signature is formed which contains characteristics of the original work, as well as the identity of the author.

As described in this publication, such a signature can be transmitted concurrently with the data of the original work or also be hidden therein in such a way that it also serves the purpose of a watermark. Also, as described in this publication, the digital watermark can additionally be provided with an authentic time stamp.

U.S. Patent No. 5,499,294 also describes generating a digital signature, which is associated with an original image and which encompasses both a hash value as well as a private key. However, this signature is not used in a watermark.

U.S. Patent No. 5,809,160 describes a method for embedding signature information in original data as watermarks, however, without mentioning a hash function.

In addition, the abstracts of German Patent Application No. 196 15 301 and European Patent 0 845 758 A3 describe embedding a digital signature in data that need to be able to be authenticated, in each case a key or a secret key being combined with an extract of the data to form an embedded signature.

Digital watermarks make it possible for a copyright owner to prove that an illegally disseminated document is his or her intellectual property. However, digital watermarks do not make it possible to determine who the originator of the illegal dissemination is, nor to prove that such a person did in fact illegally disseminate the document. This is because, in contrast to electronic fingerprints, digital watermarks do not contain any indication of an authorized recipient of a copy of the document. If such a recipient himself wants to further disseminate the document and appear to be the originator, he can likewise provide the document with his digital watermark. This can lead to the paradoxical situation in a legal dispute that both opposing parties can verify their watermark in the document at issue and each one can accuse the other of the unauthorized copy.

In such a case, the court can only pass correct judgment when the true originator can also prove a document that does not have either watermark or that only has his watermark, and not that of the opposing party. However, it can be impossible to provide such a proof, especially when working with very voluminous documents that are only available in one copy provided with a digital watermark, on one publicly accessible server.

Summary of the Invention

The present invention enables the true originator to verify his intellectual property, beyond any dispute, even in such difficult cases.

This is rendered possible by the method as set forth herein. In an embodiment, the method provides for generating digital watermarks for electronic documents, where the owner of a document hides a digital watermark as proof of identity id in the document. Prior to being hidden, the watermark is not only provided with the proof of identity id, but also at least with the hash value h(m) of the document, and with a secret key for making the watermark visible. To verify true authorship, the embodiment further allows that the reversibly embedded watermark(s) are removed again with the assistance of the secret key(s) in order to restore the document to its original state, i.e., to check it on the basis of its hash values. The method is reversible and the digital watermark can be separated again from the documents for purposes of checking the identity of the owner.

In a further embodiment, prior to being hidden, the digital watermark is not only provided with the proof of identity id, but also with an authentic time stamp, which, besides the time value t, also contains at least the hash value h(m) of the document, and, in addition, defines the embedding sequence. This method is further refined to be even more secure to enable proof of third-party attacks to be established.

In a further embodiment, to check the ownership of an electronic document in which a plurality of different watermarks were embedded, all embedded watermarks are removed, for example, under consideration of the embedding sequence, and the hash value of the thus created document is subsequently generated, which is compared to the individual hash values in the different watermarks in order to determine the original owner.

Detailed Description

In accordance with the present invention, the watermark is no longer solely dependent upon the identity id of the owner, but is additionally dependent upon document m. For this, a hash value h(m) of document m is generated, and the watermark (id, h(m)) is hidden in the document in accordance with the underlying idea in such a way that, when the watermark is removed, document m can be restored to its original state.

If an attacker were, at this point, to follow the same strategy as described above, the following would occur:

- The true originator A files document m' on a server that one obtains when one inserts watermark (a,h(m)) in m.
- An attacker B manipulates this document to m'' by additionally inserting the watermark (b,h(m')) in m'.
- At this point, the court can render a decision in the proceeding by asking the two opposing parties to reveal their watermarks (a) and to then (b) remove them from the document. The court can then calculate the hash value h(m) from the watermark-free document m and check in which of the two watermarks this value is contained.
- Alternatively or additionally, the court could also ask each of the two opposing parties to remove his or her watermark and then, from the two different documents m' and m*, calculate the hash values and check in which watermark these hash values are contained.

A further embodiment of the method is based on an authentic time stamp also being entered into the watermark. In this context, such an authentic time stamp is a time value t, together with additional information x, which was provided by an independent institution with a digital signature, for instance in the form of sig(t,x).

In this case, the watermark to be introduced into the document includes an authentic time stamp, where the additional information includes at least the hash value h(m) of document m, and the identity of the owner, e.g., in the forms: (a,sig(t,h(m))) or sig(t,(a,h(m))).

Abstract

Verification of true authorship on the basis of digital watermarks is described. The digital watermark can be provided with the proof of identity id and/or with the hash value h(m) of the document and/or with a time value t.

A METHOD FOR GENERATING DIGITAL WATERMARKS FOR ELECTRONIC DOCUMENTS

The present invention is directed to a method of the type elucidated in the definition of the species in Claim 1, as described in the postscript, JPEG, MPEG-1.

Documents which exist in electronic form can be copied as often as desired without loss of quality. For that reason, the most reliable possible methods must be employed to prevent such documents from being freely disseminated without control, in order to protect the rights of the intellectual property owner.

Due to the rapid growth of the Internet and the capability it provides for digitally disseminating documents, there is an increased requirement to protect against the illegal dissemination of documents and, thus, to protect a copyright owner from pirated copies.

For this reason, large firms, such as IBM, NEC and Microsoft, and smaller firms as well, such as Digimarc (see Funkschau 17/97; p. 21) and research institutes, such as the Fraunhofer Company IGD and the GMD Darmstadt, are working on embedding so-called digital watermarks in documents. In methods having such a basis, information identifying the copyright owner is introduced as invisible information into the documents to be protected. It is hidden in the document in such a way that no outsider can discover it. Only the owner himself can make the watermark visible by using his secret key and, therefore, in the case of a legal dispute, for example, prove that he is actually the owner.

There can be different kinds of inserted digital watermarks and, in this context, each can depend on the particular type of document (e.g., postscript, JPEG, MPEG-1).

Thus, for example, from Schneider, M. et al., in the essay: "ROBUST CONTENT BASED DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION" in Proc. Intl. Conference on Image Processing (ICIP) New York, U.S., IEEE, 1996, pp. 227-230, a method is known for embedding digital signatures as hidden signatures into the useful data for verifying the authenticity of data, i.e., proving that the data have been manipulated with, in that signatures are extracted using hash functions, and the result is combined with a private key, so that, altogether, a signature is formed which contains characteristics of the original work, as well as the identity of the author.

In accordance with this publication, such a signature can be transmitted concurrently with the data of the original work or also be hidden therein in such a way that it also serves the purpose of a watermark. Also, in accordance with this publication, the digital watermark can additionally be provided with an authentic time stamp.

U.S. 5,499,294 also describes generating a digital signature, which is associated with an original image and which encompasses both a hash value as well as a private key. However, this signature is not used in a watermark.

U.S. 5,809,160 describes a method for embedding signature information in original data as watermarks, however, without mentioning a hash function.

In addition, the abstracts of DE 19 615 301 Al and EP 0 845 758 A3 describe embedding a digital signature in data that need to be able to be authenticated, in each case a key or a secret key being combined with an extract of the data to form an embedded signature.

Digital watermarks make it possible for a copyright owner to prove that an illegally disseminated document is his or her intellectual property. However, digital watermarks do not make it possible to determine who the originator of the illegal dissemination is, nor to prove that such a person did in fact illegally disseminate the document. This is because, in contrast to electronic fingerprints, digital watermarks do not contain any indication of an authorized recipient of a copy of the document. If such a recipient himself wants to further disseminate the document and appear to be the originator, he can likewise provide the document with his digital watermark. This can lead to the paradoxical situation in a legal dispute that both opposing parties can verify their watermark in the document at issue and each one can accuse the other of the unauthorized copy.

In such a case, the court can only pass correct judgment when the true originator can also prove a document that does not have either watermark or that only has his watermark, and not that of the opposing party. However, it can be impossible to provide such a proof, especially when working with very voluminous documents that are only available in one copy provided with a digital watermark, on one publicly accessible server.

The object of the present invention is to enable the true originator to verify his intellectual property, beyond any dispute, even in such difficult cases.

This is rendered possible by the method as set forth in the characterizing part of Claim 1, because the method is reversible and, thus, the digital watermark can be separated again from the documents for purposes of checking the identity of the owner.

In the characterizing part of Claim 2, this method is further refined to be even more secure to enable proof of third-party attacks to be established, and, with the characterizing part of Claim 3, the checking procedure is explained for a plurality of watermarks.

The present invention is elucidated further on the basis of the following exemplary embodiments:

In accordance with known methods mentioned, the watermark is no longer solely dependent upon the identity id of the owner, but is additionally dependent upon document m. For this, a hash value h(m) of document m is generated, and the watermark (id, h(m)) is hidden in the document in accordance with the underlying idea in such a way that, when the watermark is removed, document m can be restored to its original state.

If an attacker were, at this point, to follow the same strategy as described above, the following would occur:

1. The true originator A files document m' on a server that one obtains when one inserts watermark (a,h(m)) in m.
2. An attacker B manipulates this document to m'' by additionally inserting the watermark (b,h(m')) in m'.
3. At this point, the court can render a decision in the proceeding by asking the two opposing parties to reveal their watermarks (a) and to then (b) remove them from the document. The court can then calculate the hash value h(m) from the watermark-free document m and check in which of the two watermarks this value is contained.
4. Alternatively or additionally, the court could also ask each of the two opposing parties to remove his or her watermark and then, from the two different documents m' and m*, calculate the hash values and check in which watermark these hash values are contained.

The mentioned further refinement of the method is based on an authentic time stamp also being entered into the watermark. In this context, such an authentic time stamp is a time value t, together with additional information x, which was provided by an independent institution with a digital signature, for instance in the form of sig(t,x).

In this case, the watermark to be introduced into the document includes an authentic time stamp, where the additional information includes at least the hash value h(m) of document m, and the identity of the owner, e.g., in the forms: (a,sig(t,h(m))) or sig(t,(a,h(m))).

What is claimed is:

1. A method for generating digital watermarks for electronic documents, where the owner of a document hides a digital watermark as proof of identity id in the document, prior to being hidden, the watermark being not only provided with the proof of identity id, but also at least with the hash value h(m) of the document, and with a secret key for making the watermark visible,
characterized in that, to verify the true authorship, the reversibly embedded watermark(s) are removed again with the assistance of the secret key(s) in order to restore the document to its original state, i.e., to check it on the basis of its hash values.

2. The method as recited in Claim 1, characterized in that, prior to being hidden, the digital watermark is not only provided with the proof of identity id, but also with an authentic time stamp, which, besides the time value t, also contains at least the hash value h(m) of the document, and, in addition, defines the embedding sequence.

3. The method as recited in Claim 1, characterized in that, to check the ownership of an electronic document in which a plurality of different watermarks were embedded in accordance with Claim 1, all embedded watermarks are removed, preferably under consideration of the embedding sequence, and the hash value of the thus created document is subsequently generated, which is compared to the individual hash values in the different watermarks in order to determine the original owner.

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **A METHOD FOR GENERATING DIGITAL WATERMARKS FOR ELECTRONIC DOCUMENTS**, the specification of which was filed as International Application No. PCT/EP99/06187 on August 23, 1999 and filed as a U.S. application having Serial No. 09/807235 on April 9, 2001 for Letters Patent in the U.S.P.T.O.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
198 47 943.3	Fed. Rep. of Germany	09 October 1998	Yes

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004
CUSTOMER NO. 26646

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Joerg SCHWENK**

Inventor's Signature: Jörg Schwenk

Date: 5. June 2001

Residence: Suedwestring 27
D-64807 Dieburg
Federal Republic of Germany DEX

Citizenship: German

2-00

Inventor: **Friedrich TOENSING**

Inventor's Signature:

Date: 01/06/06

Residence: Zum Hartberg 15
D-64739 Hoechst
Federal Republic of Germany DEX

Citizenship: German

Post Office Address: Same as above.